ムラタ ホトン H15.1.25

出願先へ送付済

整理番号　２０８７１

発送番号　３７２５８８　1/　1/25

発送日　平成１５年１１月１１日　ｵｸﾘﾄ

300213390

1/10 キケン

拒絶理由通知書

JAPANESE OFFICE ACTION (mailed November 11, 2003)
Issued for Japanese Patent Application No. 2000-016354

特許出願の番号	特願２０００－０１６３５４
起案日	平成１５年１０月２０日
特許庁審査官	青木　重徳　４２２９　５Ｍ００
特許出願人復代理人	河野　英仁　様
適用条文	第２９条柱書、第２９条第２項、第３６条、第３７条

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

【Ａ】この出願は、下記の点で特許法第３７条に規定する要件を満たしていない。

記

特定発明である本願請求項１に係る発明は、特定情報に応じて取り出した対称行列の一部の成分にエンティティ固有の乱数を合成することで該エンティティ固有の秘密鍵を生成する方法について記載したものであるのに対し、本願請求項９に係る発明は、秘密鍵から共通鍵を生成する方法について記載したものであり、これら両発明の主要機能及び解決しようとする技術課題が異なっていることから、本願特許請求の範囲に記載されているものは、特許法第３７条に規定する要件を満たしていない。

この出願は特許法第３７条の規定に違反しているので、請求項１－８，１０－１５以外の請求項に係る発明については同法第３７条以外の要件についての審査を行っていない。

【Ｂ】この出願の下記の請求項に係る発明は、下記の点で特許法第２９条第１項柱書に規定する要件を満たしていないので、特許を受けることができない。

記

・請　求　項：１－７
・備　　考

計算法、作図法と認められる発明は、一般に人間の推理力や記憶力を利用するものであって自然法則利用の技術的手段を伴うものでないから、特許法第２条に

C.添　　20871

定義されている発明とは認められず、同法第２９条の特許要件を備えていないと解するのが原則である。

そして本願請求項１－７に係る発明は、秘密鍵をどのような計算処理により生成するか、その計算法を定義したものであるから前記原則が適用できる。

・請　求　項：８
・備　　考

文字、数字、記号などを適当に組み合わせて暗号を作成する方法の発明は、たとえ産業上、殊に商取引において貢献するところが大であり、また作成方法が科学的に精密を極めていても、その間何らの装置を用いず、自然法則利用の技術的手段を施していないから、特許法第２条に定義されている発明と認められず、特許法第２９条の特許要件を備えていないと解するのが原則である。

そして、本願請求項８に係る発明は、秘密鍵から生成した共通鍵によって平文を暗号化する方法、つまり暗号を作成する方法について定義したものであるから、上記原則を適用できる。

・請　求　項：１０
・備　　考

計算法、作図法と認められる発明は、一般に人間の推理力や記憶力を利用するものであって自然法則利用の技術的手段を伴うものでないから、特許法第２条に定義されている発明とは認められず、同法第２９条の特許要件を備えていないと解するのが原則である。

そして本願請求項１０に係る発明は、秘密鍵からどのようにして共通鍵を生成するか、その計算法を定義したものであるから前記原則が適用できる。

・請　求　項：１１，１２
・備　　考

文字、数字、記号などを適当に組み合わせて暗号を作成する方法の発明は、たとえ産業上、殊に商取引において貢献するところが大であり、また作成方法が科学的に精密を極めていても、その間何らの装置を用いず、これを暗号による通信方法と解しても暗号による思想表現の方法と認められ、自然法則利用の技術的手段を施していないから、特許法第２条に定義されている発明と認められず、特許法第２９条の特許要件を備えていないと解するのが原則である。

そして、本願請求項１１，１２に係る発明は、秘密鍵から共通鍵を生成して暗号通信を行う方法について記載したものであるから、上記原則が適用できる。

・請　求　項：１３
・備　　考

文字、数字、記号などを適当に組み合わせて暗号を作成する方法の発明は、た

とえ産業上、殊に商取引において貢献するところが大であり、また作成方法が科学的に精密を極めていても、その間何らの装置を用いず、これを暗号による通信方法と解しても暗号による思想表現の方法と認められ、自然法則利用の技術的手段を施していないから、特許法第２条に定義されている発明と認められず、特許法第２９条の特許要件を備えていないと解するのが原則である。

してみると、本願請求項１３に係る発明は「暗号通信システム」について記載したものであるから、上記原則にはあたらないとも考えられるが、各請求項において暗号通信システムに用いるハードウェア資源は何ら定義しておらず、実質的な記載内容が暗号通信を行う方法について記載したものであることを勘案すれば、上記原則を類推適用できる。

よって、本願請求項１３に係る発明はその間何らの装置も用いておらず自然法則を利用した技術思想の創作にはあたらないことから、特許法第２条でいう「発明」には該当せず、同法第２９条の特許要件を備えていない。

【C】この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第２号に規定する要件を満たしていない。

記

本願請求項１４，１５に係る発明の記録媒体は、記録対象となるプログラムにプログラムコード手段を含む構成となっているが、本来記録媒体に記録されるものはソフトウェアであることを勘案すれば、前記プログラムコード手段がハードウェアなのかソフトウェアなのかが、そのカテゴリーが不明であるため、発明の内容が不明確である。

よって、請求項１４，１５に係る発明は明確でない。

【D】この出願の下記の請求項に係る発明は、その出願前日本国内において頒布された下記の刊行物に記載された発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　　（引用文献等については引用文献等一覧参照）

・請　求　項：１－７
・引用文献等：１，２
・備　　考

引用文献１には、買収結託による乱数置換攻撃を回避するために、分割ブロックが独立して攻撃されないような工夫として、エンティティの個人秘密乱数をＩＤ分割ベクトルに対応した成分に合成して前記エンティティ固有の秘密鍵を生成する方法が記載されている。

引用文献２には、鍵生成のパラメータをサブセンタが他のサブセンタとは独立

して設定することができるとともに、乱数の消去技術としてハッシュ値の部分系列を誤り訂正符号の符号語で構成し、これら複数個の符号の組み合わせで乱数を消去する技術が開示されている。

そして、引用文献１，２が共に第四の鍵共有方式について記載したものである点を勘案すれば、引用文献１に記載されている方法において、引用文献２に記載されているものを採用し、乱数パラメータをハッシュ値等により各センタで独立して設定できるようにすることは、当業者が容易になし得たことである。

・請　求　項：８
・引用文献等：１，２
・備　　考

引用文献１には、買収結託による乱数置換攻撃を回避するために、分割ブロックが独立して攻撃されないような工夫として、エンティティの個人秘密乱数をＩＤ分割ベクトルに対応した成分に合成して前記エンティティ固有の秘密鍵を生成し、該秘密鍵に基づいて通信相手エンティティとの共通鍵を生成し平文を暗号化する方法が記載されている。

引用文献２には、鍵生成のパラメータをサブセンタが他のサブセンタとは独立して設定することがでるとともに、乱数の消去技術としてハッシュ値の部分系列を誤り訂正符号の符号語で構成し、これら複数個の符号の組み合わせで乱数を消去する技術が開示されている。

そして、引用文献１，２が共に第四の鍵共有方式について記載したものである点を勘案すれば、引用文献１に記載されている方法において、引用文献２に記載されているものを採用し、乱数パラメータをハッシュ値等により各センタで独立して設定できるようにすることは、当業者が容易になし得たことである。

・請　求　項：１０－１５
・引用文献等：１，２
・備　　考

引用文献１には、買収結託による乱数置換攻撃を回避するために、分割ブロックが独立して攻撃されないような工夫として、エンティティの個人秘密乱数をＩＤ分割ベクトルに対応した成分に合成して前記エンティティ固有の秘密鍵を生成し、生成された一方のエンティティ固有の各秘密鍵に含まれている通信相手エンティティに対応する成分をそれぞれ取り出し、取り出した成分をＸＯＲ合成して共通鍵を生成して暗号通信を行うことが記載されている。

引用文献２には、鍵生成のパラメータをサブセンタが他のサブセンタとは独立して設定することがでるとともに、乱数の消去技術としてハッシュ値の部分系列を誤り訂正符号の符号語で構成し、これら複数個の符号の組み合わせで乱数を消去する技術が開示されている。

そして、引用文献１，２が共に第四の鍵共有方式について記載したものである

点を勘案すれば、引用文献１に記載されている方法において、引用文献２に記載されているものを採用し、乱数パラメータをハッシュ値等により各センタで独立して設定できるようにすることは、当業者が容易になし得たことである。

また、これら暗号通信をコンピュータ端末間で実現するために、引用文献１，２に記載されている機能をプログラム化して前記コンピュータ端末の記録媒体に記録しておくことは、当業者にとって常套手段である。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

引　用　文　献　等　一　覧

１．辻井重男，村上恭通，笠原正雄，“第四の鍵共有方式－拡張ＩＤ－ＮＩＫＳの提案”，１９９９年暗号と情報セキュリティシンポジウム予稿集，日本，１９９９年　1月２６日，Ｖｏｌｕｍｅ　１　ｏｆ　２，ｐ．１３５－１４０

２．笠原正雄，村上恭通，辻井重男，“３層構造を有する鍵共有方式の提案”，電子情報通信学会技術研究報告（ＩＳＥＣ９９－２），日本，社団法人電子情報通信学会，１９９９年　５月２０日，Ｖｏｌ．９９，Ｎｏ．５７，ｐ．９－１３

－－－－－－－－－－－－－－－－－－－－－－－－－－－－

先行技術文献調査結果の記録

・調査した分野　　ＩＰＣ第７版
　Ｈ０４Ｌ９／０８

・先行技術文献
　特開２０００－３３２７４４号公報

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。